Qualys Data + Splunk Security Analytics = Finding Hidden Threats

Don Leatham

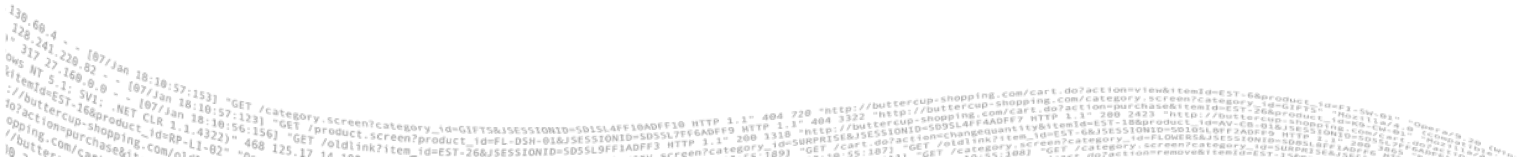
Splunk Global Strategic Alliances | Security Markets

splunk>

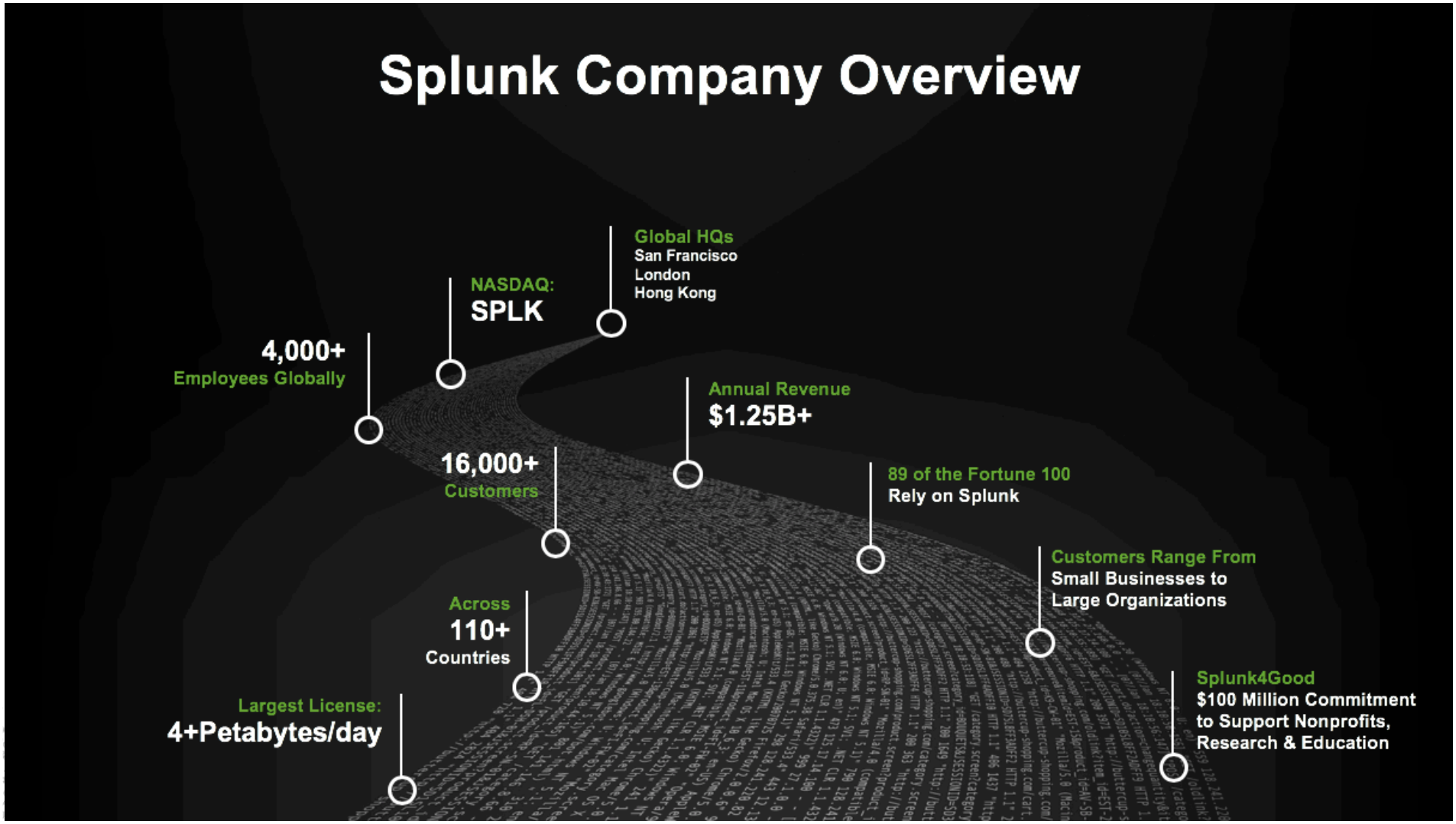
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.



splunk> listen to your data


Splunk Company Overview
Global HQs
San Francisco
London
Hong Kong
NASDAQ:
SPLK
4,000+
Employees Globally
Annual Revenue
$1.25B+
16,000+
Customers
89 of the Fortune 100
Rely on Splunk
Customers Range From
Small Businesses to
Large Organizations
Across
110+
Countries
Largest License:
4+Petabytes/day
Splunk4Good
$100 Million Commitment
to Support Nonprofits,
Research & Education

Finding Answers You Need to Take Action

IT Operations

How do I predict service-level degradation before it occurs?

Application Analytics

Is my poor app performance due to code-level errors or infrastructure?

Security and Compliance

How can I speed up security investigations and reduce the impact of insider threats?

Business Analytics

Do my marketing campaigns drive more orders through the website or mobile app?

Internet of Things

How can I monitor and analyze data from tens of thousands of sensors in real time?

ING

Adobe

SEAL OF THE CITY AND COUNTY OF SAN FRANCISCO

Domino's

BOSCH

splunk> listen to your data

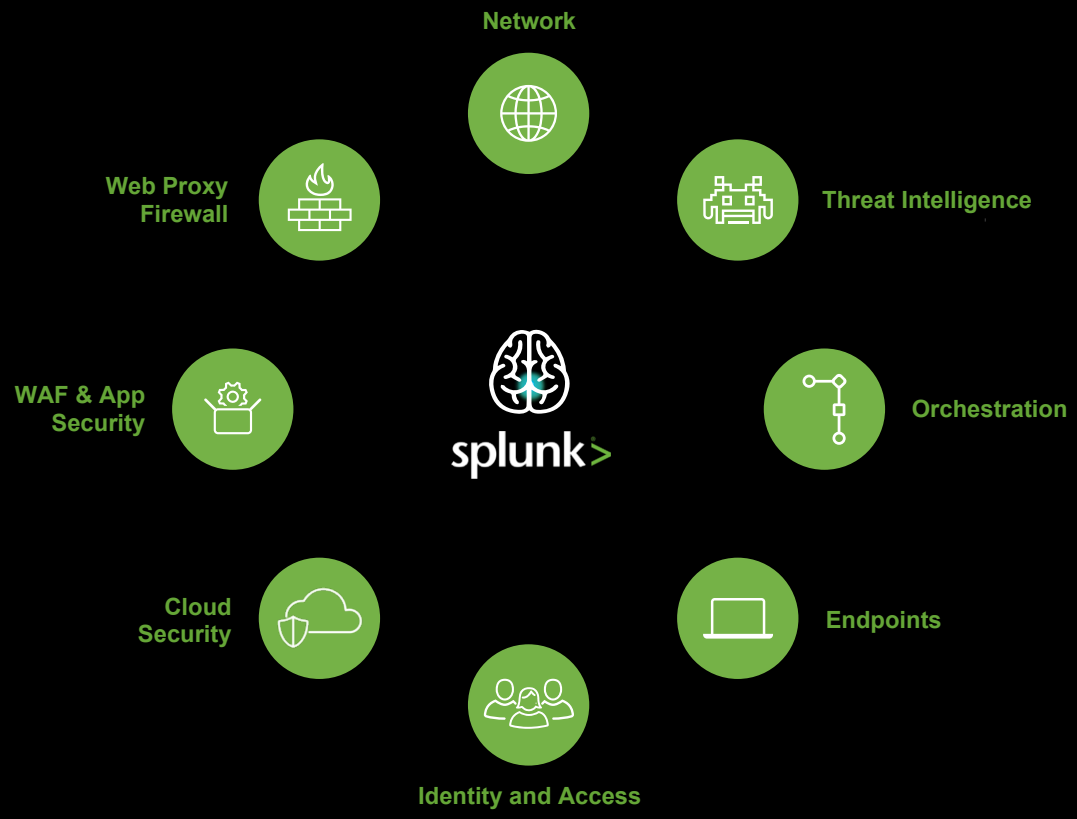
Trusted by Brands Around the World, Supported by a Deep Ecosystem

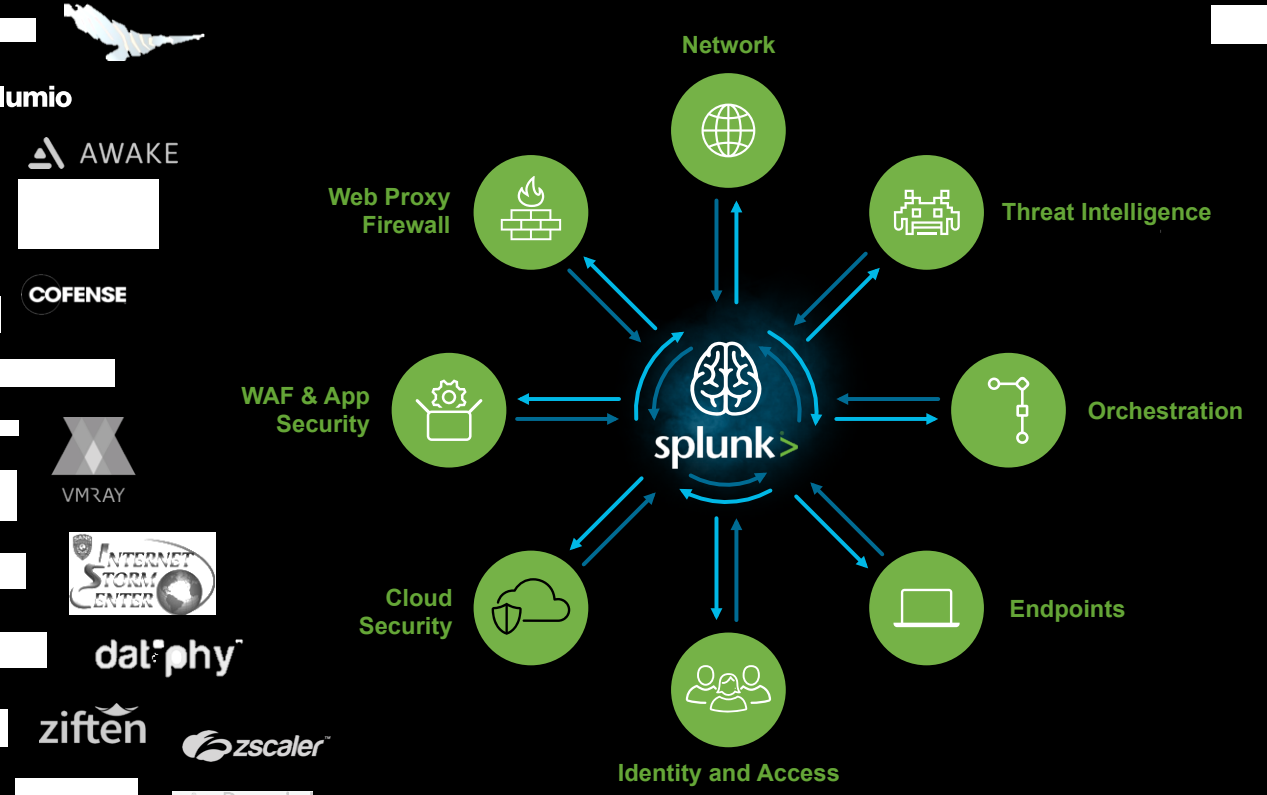
IT Operations	App Analytics	Security & Compliance	Business Analytics	Internet of Things
yelp, intuit, WORLD BANK GROUP	NORDSTROM, FamilySearch, AAA Insurance, CSAA Insurance Group	BLACKROCK, ASU Arizona State University, First Data.	UNLV, Domino's, SHAZAM	Gatwick, McKenney's, BOSCH Invented for life
syncsort, DELL EMC	puppet, New Relic.	Symantec., cisco, paloalto	+ableau, box, TEALIUM	OSIsoft., kepware, TRIDIUM

splunkbase™

splunk> listen to your data

Security Nerve Center





illumio
AWAKE
COFENSE
VMRAY
Internet Storm Center
datophy
ziften
zscaler
Recorded Future

LogicHub
netskope
Pinn AuthX
cisco
SYNCURITY
TCELL
SentinelOne
graphistry
accenture

splunk> listen to your data

Splunk Security Nerve Center Portfolio

DATA PLATFORM

splunk>enterprise

splunk>cloud

splunk>base

ANALYTICS

splunk> essentials for Security

Splunk Enterprise Security™

Splunk User Behavior Analytics™

OPERATIONS

splunk> phantom

Splunk Enterprise Security™

Phantom Community

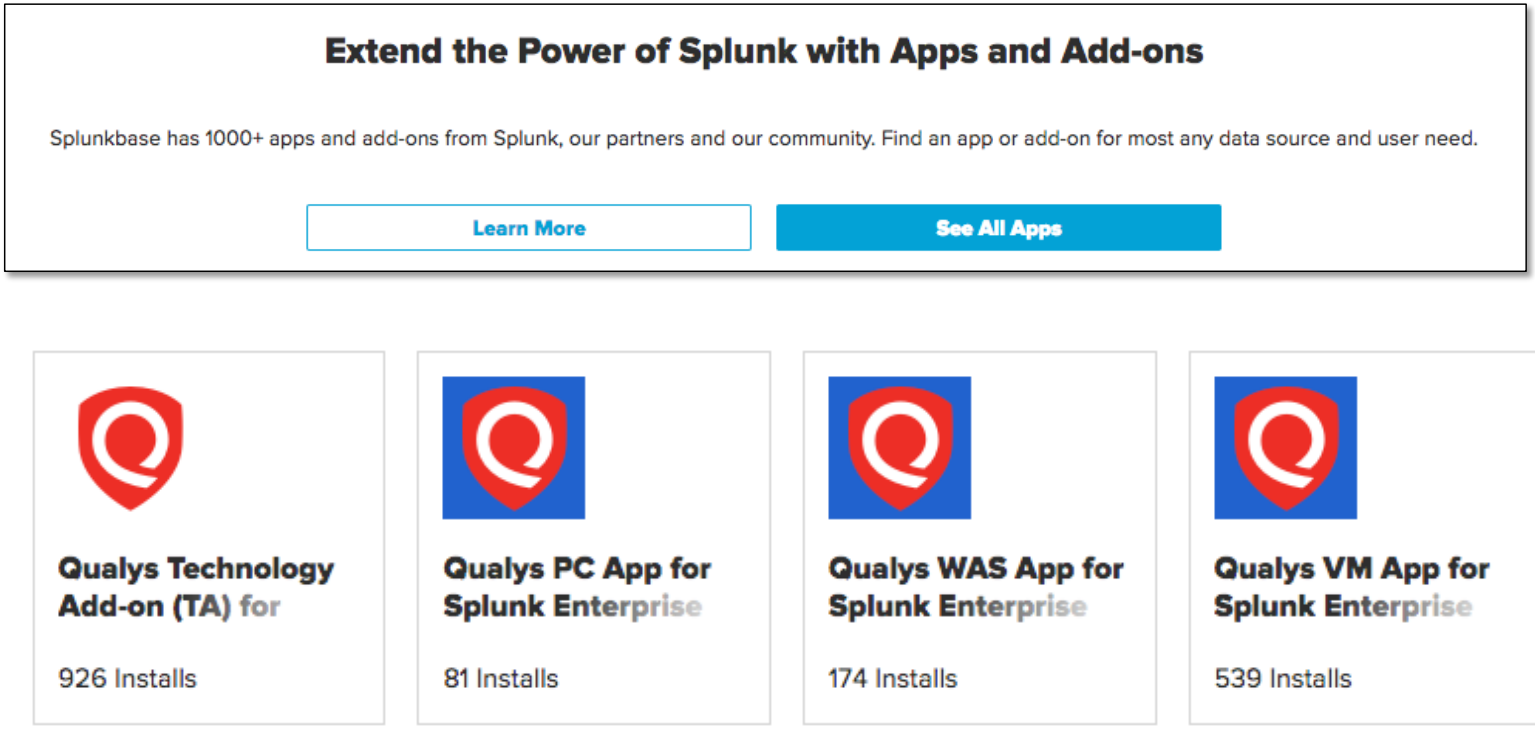
splunk> listen to your data

Qualys Integrations with Splunk Enterprise

Leveraging Qualys-Derived Data to Uncover Security Threats

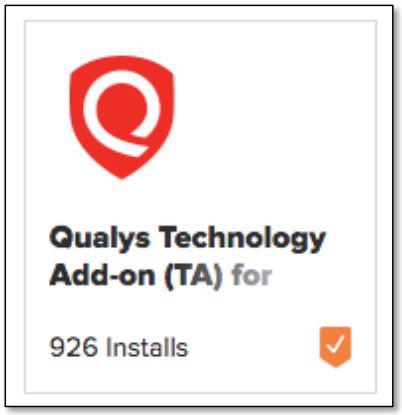
splunk> listen to your data

Splunkbase.com – Qualys Splunk Apps



Qualys Technology Add-On for Splunk

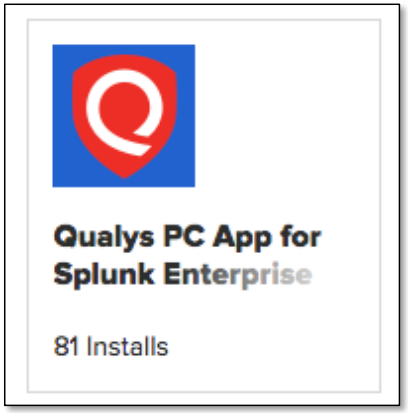
- Fetches VM, WAS, PC and KB data
- Indexes the data for search within Splunk Enterprise Security
- Supports: Qualys VM App, WAS App, PC App running on Splunk enterprise

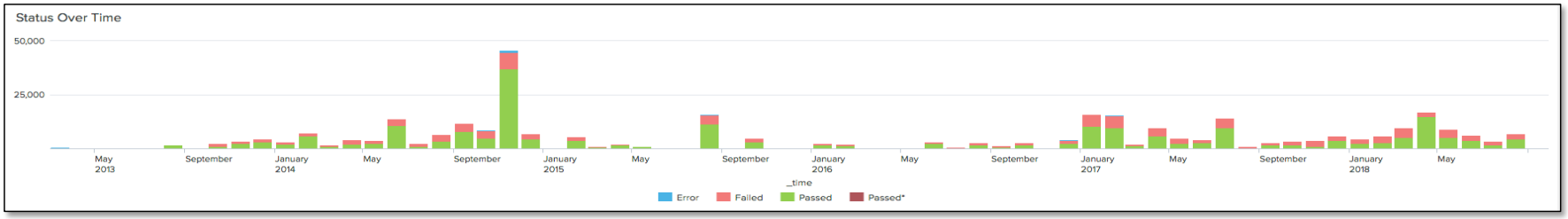


Qualys PC App for Splunk Enterprise

Searches PC data for:

- Top 10 Least Compliant Hosts
- Top 10 Policies with Failing Controls
- Policies Not Evaluated in the Last 10 Days
- And lots more via custom SPL queries

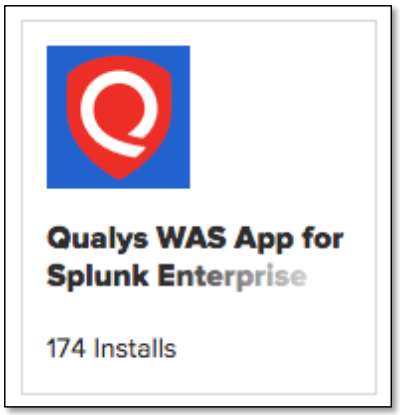


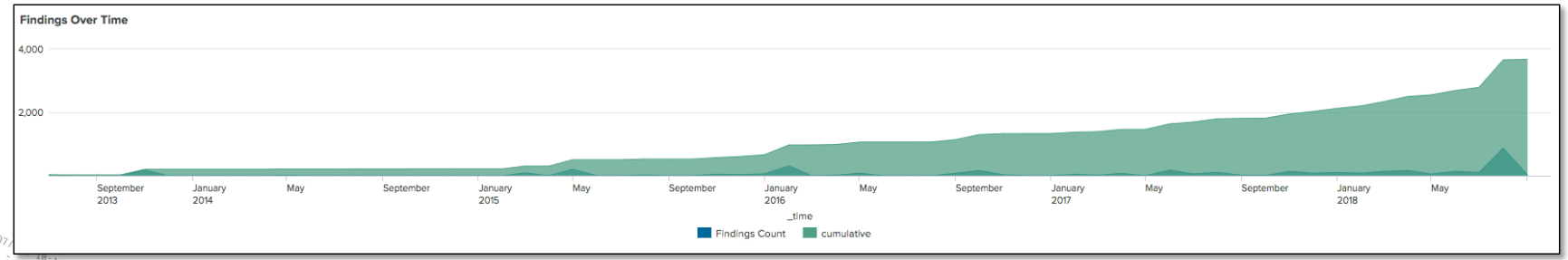


Qualys WAS App for Splunk Enterprise

Searches WAS data for:

- Total Web Application Count
- Total Findings by Severity Level
- OWASP Top 10
- Total Findings by Application
- And lots more via custom SPL queries



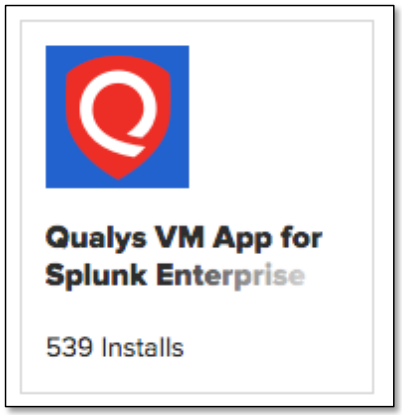


splunk> listen to your data

Qualys VM App for Splunk Enterprise

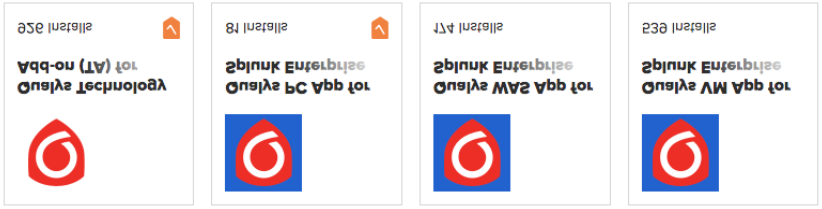
Searches VM data for:

- Total Host Count
- Top Ten Hosts – Active w Sev5 Vulns
- Most Prevalent Vulnerabilities
- Hosts Not Scanned in More Than 30 Days
- And lots more via custom SPL queries



splunk> listen to your data

Qualys– Splunk Roadmap



- Qualys apps for Splunk will be made open source
- Customizable to meet customers' exact needs
- Splunk/Qualys community will contribute additional searches and dashboards to cover a wider range of use cases

splunk> phantom

- Qualys App for Splunk Phantom
- Automated playbooks that can orchestrate key Qualys functionality
- Include Qualys "actions" as part of powerful, multi-vendor automated responses to attacks and threats

Thank You

splunk>